[GeoApps und Datenschutz am eigenen Smartphone](https://www.eduacademy.at/gwb/course/view.php?id=938" \l "section-23)

Resümee

Um eine Reflexion zum persönlichen Umgang mit Apps und sensiblen Daten zu ermöglichen, bedarf es zuerst einer grundlegenden Analyse des Verhaltens auf Internet fähigen mobilen oder stationären Endgeräten.

Meine Hauptgeräte sind das Mac Book Pro der Generation 2015, sowie das iPhone XR der Generation 2018. Beide Geräte verfügen über das Mac OSX bzw. IOS Betriebssystem aus dem Hause APPLE, welches nach wie vor für eine sehr sichere Betriebssoftware bekannt ist. Nichtsdestotrotz sind auch Geräte dieser Kategorie vor Schadsoftware, Trojanern, oder kurz gesagt vor Menschen, die sensible Daten durch Tricks jeglicher Art abgreifen wollen, gefeit. Um dieses Risiko ebenfalls zu minimieren, ist der Umgang mit den Geräten entscheidend.

Durch die gute Zusammenarbeit beider Geräte ist oftmals die Passworteingabe bei verschiedensten Seiten zum einfachsten Akt der Welt geworden. Da das iPhone über eine sehr gute und vor allem genaue Gesichtserkennungssoftware verfügt, werden fast alle Passwörter in der sogenannten iCloud Keychain gespeicehrt und verwaltet. Das bedeutet, der Zugriff zum gespeicherten Passwort wird erst erlaubt, nachdem das Gerät sichergestellt hat, dass es sich um mich selbst als Nutzer handelt. Zugegebenermaßen gleichen, oder ähneln sich viel meiner Passwörter. Dies ist jedoch auf banale Bereiche wie etwa SocialMedia oder Spieledienste bzw. Universitätsdienste beschränkt. Wichtige Zugänge, wie etwa der Bank Zugang sind nicht gespeichert in der iCloud Keychain und müssen daher jedes Mal manuell eingegeben werden. Dies gab mir bis vor Kurzem große Sicherheit. Da die Bank meines Vertrauens die Umstellung des Online Bankings auf die sogenannte Zwei Faktor Authentifizierung ausgeweitet hatte, musste ich wohl oder übel meinen Bankzugang auch auf mein Mobiltelefon ausweiten. Ich denke jedoch, dass sich auch bei Verlust oder Diebstahl des Smartphones die Sicherheitsfeatures der App bewähren und werden und daher kein Schaden entstehen wird. Jede Transaktion muss mobil mit der Gesichtserkennung bestätigt werden, bzw. stationär zusätzlich am Mobiltelefon ebenfalls mit Gesichtserkennung abgesegnet werden.

Hinsichtlich der Zugriffsrechte war ich bis dato sehr vorsichtig und ließ Apps Standort, wenn nicht notwendig nur während der Verwendung der App zu. Auch wurden andere Zugriffsrechte nur bei absoluter Notwendigkeit gewährt. Die Problematik liegt jedoch an zweierlei: der technologische Fortschritt erleichtert viele Bereiche des alltäglichen Lebens ungemein, resultiert jedoch gleichzeitig in einer gewissen Einschränkung der Privatsphäre. So gelangt man schnell in ein Dilemma. Bekannte Beispiele sind etwa der auditive Assistent Siri (Apple) oder Hey! Google (Google). Hierbei können leichte alltägliche Befehle die Gestensteuerung am Mobiltelefon ersetzen. Man muss sich jedoch darüber im Kalren sein, dass das Smartphone zu jedem Zeitpunkt Gespräche auf den Aktivierungsbefehl „Hey Siri“ mitbelauscht. Man hofft zumindest, dass sich die Gesprächsaufzeichnung darauf beschränkt.

Ich persönlich nutze den Assistenten zusammen mit den kabellosen Kopfhörern AirPods gerne, da diese Kombination eine fast gestenlose Steuerung des Handys rein durch auditiven Input ermöglicht.

Ein weiteres Beispiel ist Googles Tracking Funktion „Timeline“, welche auf hauseigenenem Kartenmaterial GoogleMaps animiert darstellt, wo sich der Benutzer an besagtem Tag bewegt hat. Diese Funktion wurde im letzten Urlaub kontrovers diskutiert, von Überwachung bis zu nützlichem Gadget waren alle Meinungen vertreten. Am Ende überwog die Neugier und auch ich gewährte der App dauerhaften Zugriff auf meinen Standort. Die gedankliche Rechtfertigung kam aus der Überlegung: „Tut Google Maps dies nicht ohnehin auch, sine mea sententia, also ohne mich zu fragen?“

Um den Bogen der Smartphone Nutzung vom psychologischen/philosophischen zurück zur Realität zu spannen, die Nutzung der Social Media Kanäle ist von Ups and Downs geprägt. Wurde zu Beginn im wahrsten Sinne des Wortes kein Gedanke an Sicherheit verschwendet, ist heute dieses Thema oberstes Gebot. Alle Like und Follower erhaschenden selbstdarstellerischen Gedanken wurden über Bord geworfen und jegliche Profile auf privat gestellt. Auch wurde das Nutzungsverhalten stark hinterfragt: „ist Social Media wirklich so wichtig, dass du mehrere Stunden täglich darauf verbringst?“ Den erschreckenden Tatsachen, welche vom Handy eigenen Dienst „Screen Time“, welcher das Nutzungsverhalten trackt, aufgedeckt wurden, nach, wurden alle Profile auf Privat gestellt, das Nutzungsverhalten reduziert und gut und gerne mal ein Buch statt dem Handy in die Hand genommen.

Was ich selbst wohl daraus gelernt habe, kann ich am Nutzungsverhalten anderer auch erkennen: vielen geht es ähnlich. Manche sind noch sehr in der Suchtspirale drin, jedoch werden auch diese irgendwann erkennen, dass Social Media nicht das Lebensglück mit sich bringt und es daher keinesfalls wert ist, sensible Daten presizugeben, nur um anderen zu gefallen.